June 22, 2013

Re: Proceeding RM-11699

Being involved in both Public Safety and Emergency Management communications I have often thought about submitting a request for rulemaking that provides specific and selective exclusions to 97.212 and 97.213 but never got beyond a draft. I support specific and selective exemptions to provide for a reasonable, yet accountable level of communications security for the "written" word, during time of specific need and with reasonable level of accountability as follows:

William Powell – WB1GOT

Permissible Instances of Encryption

§ 97.212 Encryption. (or) § 97.213 Encryption

(a) Except as otherwise prohibited herein, an amateur station operating as, or in association with a [competent / official / responsible] U. S., state, county or parish or local government agency or government [competent / official / responsible] Non Governmental Organization (NGO) both during an emergency declared by a [competent / official / responsible] governmental authority or during a government or NGO [sponsored / authorized] drill or training exercise may transmit encrypted messages.
(Permit specific instances when encryption is permissible.)

(b) Permitted Emissions / Methods:
(1) Only messages originated as human readable text and ultimately displayed as human readable text shall be permitted to be encrypted. This specifically excludes the encrypted transmission of voice and / or graphic images.
(Exclude all non "written" (hardcopy) encrypted transmissions and provide for accountability.)

(2) "Containers" used for the purpose of compressing the message for transmission assurance or for the reduction in message size shall be permitted. Examples: "ZIP" compression however the container may NOT be separately encrypted.
(3) Common file formatting such as might be used by application programs commonly found installed on home or business computers shall be permitted but may NOT be separately encrypted. Examples: .TXT, .DOC, .XLS
(Provide that ONLY the message, as a whole, be permitted encryption and specifically exclude separate (additional) content encryption.)

(c) Permitted Messages:
(1) Only those messages originated by a government agency or NGO and,
(2) Are directly related to the immediate health and safety or protection of property and,
(3) Are considered sensitive by the government agency or NGO originator and,
(4) Are required, by (U.S.) government law or statute, to be obscured or encrypted for transmission and,
(5) Have a time sensitivity or level of urgency that requires immediacy and transmission via radio as opposed to other methods,
(6) "Test" messages intended for drill and practice purposes. Such messages must be repeated in the clear (unencrypted) immediately following the encrypted transmission.
(Severely limit the types of information permitted to be encrypted.)

(d) Prohibited Messages:
The following types of messages are specifically excluded from this exception to encryption:
(1) Any message not originated by a government agency or NGO.
(2) Any message in which the content might facilitate normal business or provide for, or enable remuneration or pecuniary interest to any of the involved parties.
(3) Any message of a routine or reporting nature.
(4) Any message concerning the trivial health or welfare of an individual or group of individuals ultimately [reported / delivered] to an individual not associated with an involved Governmental Agency / NGO.
(5) Any message originated by, relayed by or intended for any non-FCC licensed station.
(6) With the exception of 97.113 (4) "messages encoded for the purpose of obscuring their meaning" any message prohibited elsewhere in this part.
(Ibid.)

(e) Encrypted Message Requirements:
Messages encrypted in accordance with this part shall be transmitted with the following minimal message header contents transmitted in the clear:
(1) Originating station FCC granted call sign,
(2) Call sign of ultimate FCC granted destination station call sign,

(3) FCC granted call sign of sending operator,
(4) Date and local time of origination,
(5) Unique message serial number,
(6) Count of the number of words in the encrypted message body,
(7) Document format,
(8) Container type.
(Provide specific level of accountability and responsibility.)

(f) Restriction of Origin and Delivery:
Encrypted messages shall not be sent to or received from any station other than FCC licensed stations; The originating station, all intermediate stations and the destination station shall be FCC licensed stations, all affiliated with a U.S. governmental agency or recognized NGO agency.
(Limit span and scope of encrypted transmissions and messages.)

(g) Message Retention:
Messages encrypted and transmitted in accordance with this part shall be retained as a complete, printed paper copy of the original unencrypted message including all header and trailer content by the originating station, for FCC inspection for a minimum of one year.
(Provides accountability and review should it become necessary.)

(h) Communications Security:
(1) No particular method of encryption, decryption or key generation shall be specified or required by this part,
(Relieve the government of responsibility and liability of mandating a particular method or methods.)

(2) Neither the encryption method nor the encryption / decryption key are required to be disclosed to any party without benefit of a duly issued court order.
(Provide limited protection against 3rd party activity to cause disclosure without intervention of the courts.)

(3) The sum of all keys (nominally the User and Session keys) shall not exceed 128 bits.
(Limit encryption to "reasonable" level of security; Diplomatic level protection is both excessive and inappropriate for the intended use.)